Composable Replaceable Security Services

New Ideas

- The security requirements of real world applications can be met through the composition of replaceable, portable, transportable and mobile security services.

- Security implemented through composable and replaceable security services can be reconfigured in response to threats or changes in security requirements.

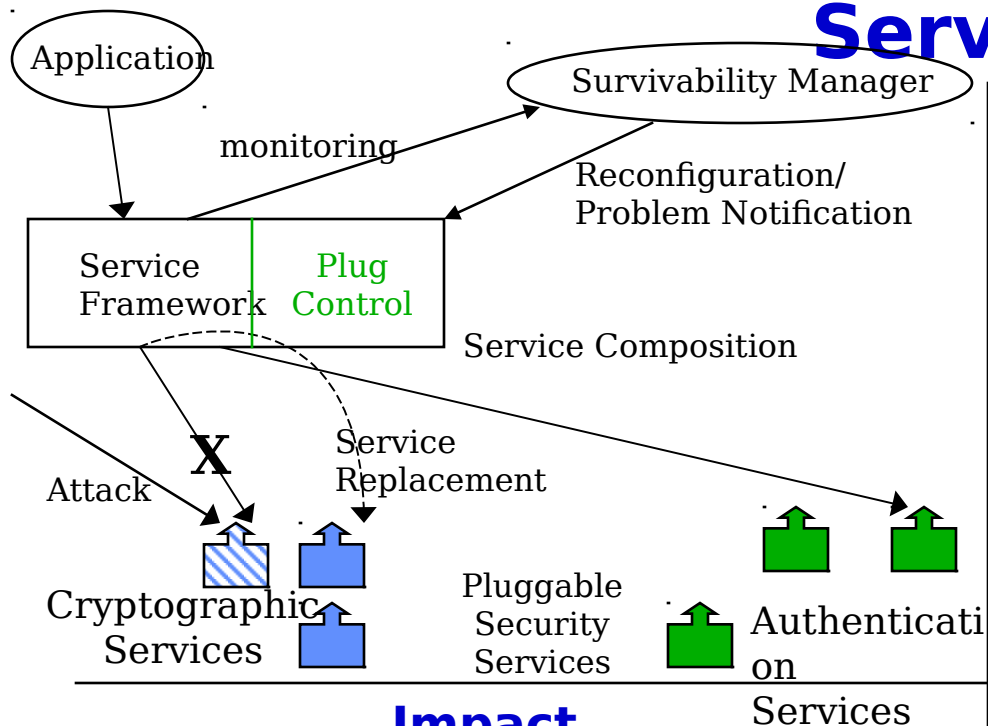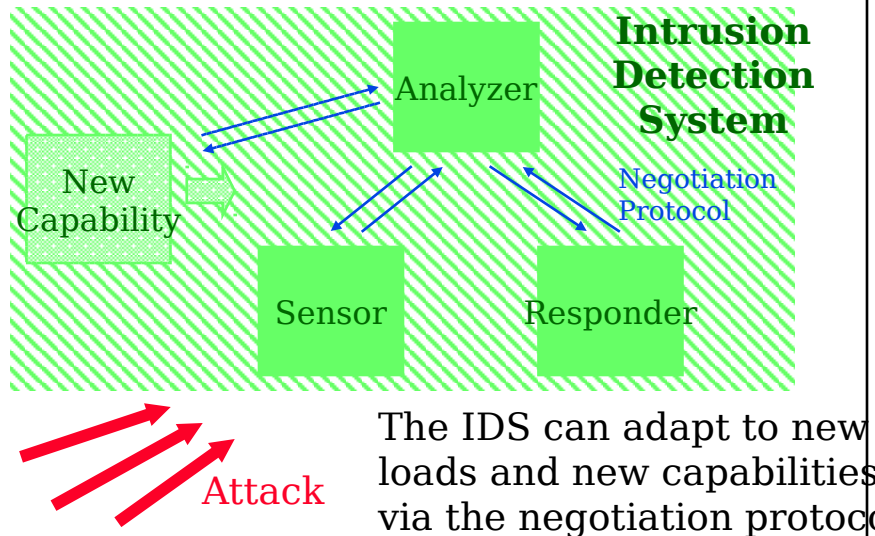- Provide a metrics-based approach to survivability monitoring, management and analysis of both systems and individual service providers.

Impact

- Provide a new paradigm for configuring and reconfiguring complex heterogeneous systems with changing components, requirements and threats.
- Provide an architecture where transparent recovery can occur after a service provider failure without any loss of data or security.
- Provide a full-fledged survivability service that can monitor survivability posture and warn system administrators when observed behavior deviates from specified survivability objectives and take corrective action such as reconfiguring to restore survivability posture.

Schedule

TASK	1998 Q1 Q2 Q3 Q4	1999 Q1 Q2 Q3 Q4	2000 Q1 Q2 Q3 Q4
Write architecture report	▲		
Develop Secure CRSS Mail	▲		
Demonstrate Survivability Manager		▲	
Final Demonstration			▲

NAI Labs, Network Associates: Richard Feiertag, Tim Redmond

INTRUSION DETECTION INTERCOMPONENT ADAPTIVE NEGOTIATION (IDIAN)

Intrusion Detection System

Analyzer

New Capability

Negotiation Protocol

Sensor

Responder

Attack

The IDS can adapt to new loads and new capabilities via the negotiation protocol.

New Ideas

• Protocol permits negotiation of a large number of complex alternatives rather than a small number of simple alternatives negotiated in existing protocols.

• Filter expressions are used to define negotiation alternatives and to guarantee that negotiations converge to a successful conclusion, if possible.

• The relative cost of alternatives is an explicit element of the negotiation.

Impact

• Enables more effective intrusion detection systems by simplifying the efficient interoperation of diverse ID components.

• Permits ID systems to rapidly adapt to changing conditions by optimizing both their functional capabilities and their resource allocation.

• Permits dynamic addition and removal of capabilities to ID systems, thereby permitting continuous operation

Schedule

TASK	1998 Q1 Q2 Q3 Q4	1999 Q1 Q2 Q3 Q4	2000 Q1 Q2 Q3 Q4
Demo Requirements Report		▲	
Initial Negotiation Protocol Design		▲	
Initial Implementation		▲	
Final Implementation			▲
Final Negotiation Protocol Spec.			▲

NAI Labs, Network Associates: Richard Feiertag, Karl Levitt, Stuart Staniford-Chen